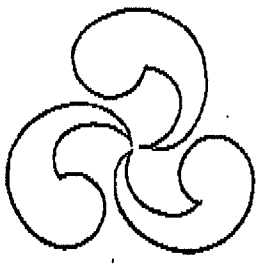
量子力学の基礎と量子暗号
量子通信チャンネルの視点



内山　智香子

1. はじめに

コンピュータネットワークをはじめとするさまざまな通信網が急速な発展を遂げている現在では，通信の機密性やプライバシーを保護するための高度な秘匿機能が要求されている．暗号はこの秘匿機能の中心的な役割を果たすもので，従来は主に外交や軍事上の目的で開発されてきたが，最近ではソフトウェアの権利保護等を含む多彩な場面で用いられるようになってきている．暗号を作成したり，安全性を論ずる際には，長い間数学的な立場からの研究が行われてきたが，1980年代に量子力学の原理を通信に用いることがウィーズナーによって提案[1]されて以来，物理学と暗号学との接点が生まれた．

ウィーズナーの提案は，2つの異なるメッセージを量子論的な光の偏光状態を用いて伝送する，というものである．まず，2つのメッセージを両方とも2進法で表わしておき，一方のメッセージについては，互いに直角な2つの直線偏光の光で，もう片方のメッセージについては右回り・左回り円偏光の光で0，1の値を表現し，光導波路に伝送する．さらに，メッセージの伝送の度毎に，2つのメッセージのうち，どちらを伝送するのかをランダムに選び出すようにしておく．このようにすれば，受信者は，偏光の性質から2つのメッセージのうちの片方は読み出せても，両方を正確に読み出すことはできない．これは次のような事情による．光の偏光方向を知るには，フィルターとなる物質に光を通せばよい．例えば，適当に切り出した方解石の結晶に光を入射すると，直進光と屈折光の2本の光が出力される．この2本の光は各々直線偏光状態にあり，その偏光方向は互いに直交している．したがって，結晶から出力される光の出力位置によって，直線偏光を用いたメッセージは確実に解読できる．しかし，円偏光の光が方解石を通過すると，円偏光であったことは失われて，直進光か屈折光かが，ある確率で出力されることになる．円偏光の光は，互いに直交した2つの直線偏光の光を一定の位相関係を持って重ね合わせたものであるので，このような現象が生じる．逆に，円偏光の向きを区別できるフィルターに直線偏光状態の光を通せば，入力前の偏光状態は失われ，右回りか左回りかの円偏光状態の光が，ある確率で出力される．これら4種類の偏光を用いた2つのメッセージが送信された場合，受信者が片方のメッセージを正確に読み取ることのできる装置をもっていたとしても，もう片方のメッセージの内容は変化してしまう，というわけである．

以上の現象は量子力学によって次のように説明されている：光は光子と呼ばれる粒子の集まりだと考えられており，光子は偏光をその属性の一つとして持っている．また，光子の各々は必ず光の振動数に応じて決まる一定量のエネルギーを持っている．この意味で，光子を1個，2個と数えることのできる「粒」とみなすことができるのである．さらに，さきほど，円偏光は互いに直角な2つの直線偏光を「重ね合わせ」たものである，と述べたが，これは「重ね合わせの原理」とよばれる量子力学の原理の一例となっている．この原理によれば，量子力学系の任意の状態は，複数の状態をある確率で重ね合わせることによってつくることができる．その意味するところを円偏光の例で述べよう．円偏光状態の光を減衰させ，円偏光の光子を方解石にあてる実験を何度も繰り返すと，互いに直角な方向に偏光した2種類の直線偏光の光子が出力される場合が各々ある確率で得られる，ということを，この原理は意味しているのである．人によっては，「円偏光は部分

的に垂直偏光であり，また部分的に水平偏光である」，という言い方をするが，いわゆる日常的に用いられている「半死半生の状態」[2]とは意味が全く違うことに注意しよう．また，円偏光の光を方解石に通すと直線偏光が出力されるのは，我々の行う観測によって光の状態が乱されてしまうことを意味している．ウィーズナーの提案は，このような光の量子論的性質を通信の際の符合化に利用したものであった．また，この提案で用いられている，量子論的な性質を持った信号をやりとりする際の通信路を，量子伝送路，あるいは，量子通信チャンネルとよぶ．

ウィーズナーによる提案を契機として，暗号学に量子力学を用いた新しい流れが起こった．これを総称して量子暗号とよぶ．その端緒となったのは，1984年のベネットとブラサードによる提案であった[3,4]．彼らは，ウィーズナーの提案を，通信内容の機密保持に応用することを考えた．彼らは，まず，ウィーズナーの用いた0と1からなる数列をメッセージではなく，暗号の作成・解読のための乱数列（これを暗号鍵と呼ぶ）と読み直した．ただし，ウィーズナーの提案では，2つのメッセージをランダムに送信することからも，読み取りの不正確さが生ずるので，この方式は用いない．また，ウィーズナーの考えた受信者を盗聴者と読み直せば，盗聴行為自体が系を乱し，通信の当事者に盗聴の有無が知れてしまう工夫が可能となる，というわけである．この画期的な提案は，今日では，通称BB84プロトコル（通信規約）と呼ばれている．ベネットとブラサードによる提案以降，量子論的な性質を暗号鍵の配布に用いる系が次々と考案され，現在，量子暗号とよばれる分野の中核をなしている．そこで，本稿ではこの量子論的な暗号鍵の配布（Quantum Key Distribution－以下，QKD－）に焦点をしぼって述べることにしよう．

ベネットとブラサードによる提案以降のQKDは，主として次のような順序で（一部は並行して）発展してきた．すなわち，

(1) BB84プロトコルを忠実に実現するための実験装置の考案[5]．これは，空気中を伝播する光の偏光状態に情報を載せるものだが，光ファイバを用いて実現しようというグループもある[6]．

(2) アインシュタイン，ポドルスキー，ローゼンによって量子力学を否定するために提案されたパラドックスをもとにしたプロトコルの考案[7,8]．このパラドックスの表わす状況は，2光子干渉実験によって実現され[9]，量子力学の正当性が確かめられている．その際の光学装置を用いた暗号系も提案されている[10,11]．

(3) 干渉計を用いて暗号鍵を作成し，送信する方法の提案[12]．光ファイバを用いた装置も作成されている[13~16]．

(2)の一部[10,11]と(3)のように，最近では干渉計を用いたものが多い．筆者らはこれまで，干渉計についての量子通信チャンネル理論の定式化[17]を行ってきたのだが，これらのプロトコルは，その理論の応用例とみなすことができる．そこで，本稿では筆者の視点も変えつつ，干渉計を用いたQKDのプロトコルについて述べることにする．まず，2節でBB84プロトコルの干渉計を用いた実現法について述べ，次に3節では，理論的な準備をした上でBB84プロトコルの仕組みを解説する．その後，1992年にベネットによって考案されたB92プロトコルと，その実現例を4節で紹介する．

2. 量子論的な暗号鍵の配布（QKD）BB84プロトコル

量子論的な暗号鍵の配布（QKD）とは，通信前には秘密情報を何も共有していない送信者（以下，アリス）と受信者（以下，ボブ）とが，0と1のランダムに並んだ数列（暗号鍵）を盗聴者（以下，イブ）に知られずに共有することである．その目的で開発されたBB84プロトコルとは，もともとは0と1の値を4種類の偏光状態で表現するものであったが，この方式は長距離通信には向かない．そこで，ベネットは光の偏光状態ではなくて光の位相を用いる装置を考えた[18]．この心臓部にはMach-Zehender（以下，MZ）干渉計という，元来は，出力光の干渉縞から入力光の性質を精密に測定するための装置[18]を用いている．MZ干

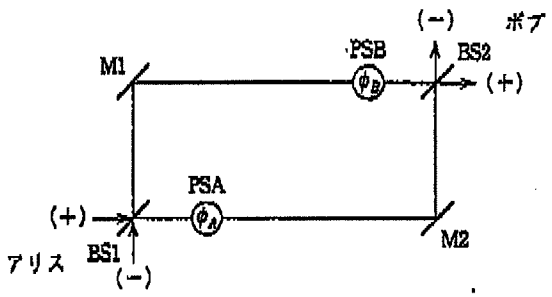


図1 Mach-Zehender干渉計

渉計は，図 1 に示すように

(1) 光を 2 方向に分けるビームスプリッタ（BS1, BS2）
(2) 光の位相を変化させる移相器（PSA, PSB）
(3) 光を全反射する鏡（M1, M2）

で構成されている．この干渉計においては，光の入力・出力は，各々2 方向からなされる．以後，BS1 に光が入力される 2 つのポートを (+), (−) とし，BS2 から出力されるポートを同様に (+), (−) とする．

さて，BB84 プロトコルがどのようにして実現されるのか，みてみよう．まず，アリスは入力側の (+) ポートから光を入射する．この光は，光子 1 つ分と考えられるほどに弱いとする．このような微弱な光を得るには，例えば，レーザー光を減衰させればよく，光を減衰させればさせるほどその量子論的な性質が強く浮き彫りになり，盗聴行為が発見されやすくなる．アリスはこのような光をある一定の間隔で入射する．具体的には，例えば 300 ps（= 100 億分の 3 秒）ぐらいのパルスをレーザーで作りだし，これを減衰させる．こうすれば，100 億分の 3 秒の間に光子が 1 回ポロッと入射することになる．また，アリスとボブは，移相器（PSA, PSB）の位相設定を独立に制御できるものとする．実際の通信手順を以下に示す．

(1) アリスとボブは 0 と 1 のランダムに並んだ数列を各自で作成する．この乱数列の長さは互いに揃えておく．例えば，アリスは $0,1,1,0,0,\cdots$，ボブは $0,1,1,1,1,\cdots$ という乱数列を作成したとしよう．
(2) アリスは，一定の時間間隔でパルス光を送信するたびに，自分の作成した乱数列に従って，移相器（PSA）で光の位相を変調する．乱数の値が 0 であれば，位相を 0 または $\frac{\pi}{2}$ とし，1 であれば，位相を π または $\frac{3\pi}{2}$ とする．(1) の例で言えば，$\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 0, \frac{\pi}{2}, \cdots$ という順番で位相設定をしたとする．
(3) ボブは，信号を受け取る直前に自分の作成した乱数列に従って移相器（PSB）の位相を変化させる．乱数列の値が 0 であれば位相を 0, 1 であれば $\frac{\pi}{2}$ とする．(1) の例で言えば，$0, \frac{\pi}{2}, \frac{\pi}{2}, \frac{\pi}{2}, \frac{\pi}{2}, \cdots$ とする．
(4) ボブの側では，どちらのポートから光が出力されるかを観測する．(+) ポートから光が出力されれば 0, (−) ポートから光が出力されれば 1 とする．光を検出したときの，ボブ側の位相の設定と，どちらのポートから光が出力されたのかを 0 か 1 かの値に置き換えたものを記録しておく．例えば，$1,0,1,0,0,\cdots$ という結果を得たとしよう．
(5) アリスが乱数列の内容をすべて送信し終わった後，お互いに設定した位相についての情報のみをアリスとボブの間で交換し，アリスとボブの設定した位相差が 0 または π のときの値のみを残す．上記の例で言えば，3 番目と 5 番目を取り出して新たな乱数列をつくり，これを暗号鍵とする．

ここで，(5) で情報を交換する際には，イブが存在していても構わない．送信前のアリスとボブの了解事項は，乱数列の 0 または 1 に割り当てられる位相の知識のみである．また，送信後は，各々の位相設定を確認するだけなのだが，両者の得る乱数列は，完全に一致している．上の (1) ～ (5) からなる第 1 回目の送受信によって全く同じ乱数が共有できていることを確認した後は，最終的に両者の得る乱数列の長さがメッセージの長さとなるまで送受信を行う．

では，なぜこのような手続きでアリスとボブが全く同じ乱数列を共有できるのだろうか？　次に，量子通信チャンネル理論を用いてこのプロトコルの仕組みを詳しく調べることにしよう．

3. 量子通信チャンネル理論

量子論的な光をやりとりする場合，MZ 干渉計は量子通信チャンネルの一種とみなされる．そこでこの節では，ビームスプリッタ，移相器といった MZ 干渉計を構成する要素の動作を記述する量子通信チャンネル理論を紹介したあと，BB84 プロトコルについて説明することにする．

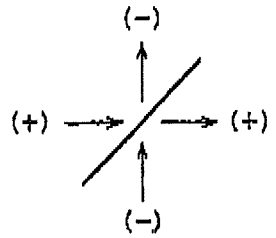


図 2　ビームスプリッタ

3.1 MZ干渉計の構成要素

まず，ビームスプリッタ（以下，BS）に注目しよう（図2）．

BSは2方向から入射された光を，反射・透過するものである．その動作を記述するために入力光の電場をフーリエ分解したときの成分（これを，複素電場振幅と呼ぶ）を用いることにする．例えば，簡単に，準単色光（振動数がほぼ1種類とみなせる光）を入力した場合は，複素電場振幅は1成分のみを考えればよい．いま，レーザーを用いて，BSの（±）ポートへ $E_{in,\pm}$ という複素電場振幅をもった準単色光を入力したとする．この複素電場振幅を要素に持つベクトル

$$E_{in} = \begin{pmatrix} E_{in,+} \\ E_{in,-} \end{pmatrix} \tag{3.1}$$

によって入力信号を表わしたとき，BSから出力される信号は，

$$E_{out} = T_{\pm} E_{in} \tag{3.2}$$

と書ける．ここで，$T_{\pm}$ は，

$$T_{\pm} = \begin{pmatrix} T & R \\ R & T \end{pmatrix} \tag{3.3}$$

という，2行2列の行列である．行列要素の R, T はともに複素量であり，$|R|^2$, $|T|^2$ が各々反射，透過率を表わす．そこで，これらは

$$|R|^2 + |T|^2 = 1 \tag{3.4}$$

という関係をみたす．後々のために，ここで，変換行列 $T_{\pm}$ を

$$T_{\pm}(\alpha) = \begin{pmatrix} \cos\left(\frac{\alpha}{2}\right) & -i\sin\left(\frac{\alpha}{2}\right) \\ -i\sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{pmatrix} \tag{3.5}$$

としておく[18]．α は，反射と透過の割合を表わすパラメータである．例えば，2方向からの入力光をそれぞれ50%の割合で反射・透過するばあい，$\alpha = \frac{\pi}{2}$ となる．

2節で述べたようにレーザー光を減衰し，量子論的な光をBSに入力する場合に話を進めよう．BSは，入力された光を反射・透過するもので，光を増幅したり，減衰したりする動作はしない．(+)ポートと(−)ポートからBSに入力された光の光子数の和は，出力時にも保存されているはずである．そこで，両方のポートからの入力（出力）光子数 $n_{\pm}$ の和 $n_+ + n_-$ が一定という条件をみたす状態を重ね合せて得られる，新たな状態に注目する．すなわち，$n_+ + n_- = N$ とかいて

$$|z; N\rangle = \sum_{m=0}^{N} \frac{(z_+)^m (z_-)^{(N-m)}}{\sqrt{m!(N-m)!}} |m, N-m\rangle \tag{3.6}$$

という状態を考える．ここで，$z = \begin{pmatrix} z_+ \\ z_- \end{pmatrix}$ である．(3.6)式中の $|m, N-m\rangle$ は，m 個の光子が(+)ポートから，$(N-m)$ 個の光子が(−)ポートから入出力される状態を表わす．$|m, N-m\rangle$ の係数は，確率振幅と呼ばれるもので，絶対値の2乗は系が状態 $|m, N-m\rangle$ をとる確率となる．(3.6)式で表わされる光がBSを通過すると確率振幅が変わる．この場合，

$$|out\rangle \equiv |z_{out}; N\rangle = |T_{\pm}(\alpha) z_{in}; N\rangle \tag{3.7}$$

となることがわかっている[17]．すなわち，量子論的な光の入出力関係においては，確率振幅の変化が変換行列 $T_{\pm}(\alpha)$ を用いて表わされる．あとは，行列の計算をするだけである．

次に，BB84プロトコルで重要な役割を果たす移相器（以下，PS）を考えよう（図3）．

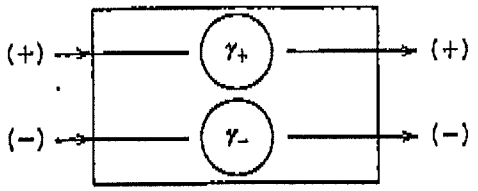


図3 移相器

これは，(+)，(−)ポートへの入力信号の位相を，γ_+, γ_- だけ変化させるデバイスである．そこで，変換行列は，

$$T_{\pm}(\gamma_+, \gamma_-) = \begin{pmatrix} e^{i\gamma_+} & 0 \\ 0 & e^{i\gamma_-} \end{pmatrix} \tag{3.8}$$

と表わされる．出力状態は，この変換行列を用いて

$$|z_{out}; N\rangle = \left| e^{-i\frac{\phi}{2}} T_{\pm}(\gamma_+, \gamma_-) z_{in}; N \right\rangle \tag{3.9}$$

となる．ここで，ϕ は

$$\phi = \gamma_+ + \gamma_- \tag{3.10}$$

である．

3.2 BB84プロトコル

これで数学的な準備が整ったので，いよいよ，BB84プロトコルの仕組みを解明することにしよう．アリスはボブに光子1つを送信するのであるから，(3.6)式

の $N=1$ の場合を取り扱うことになる．(+) ポートから 1 個の光子が入力（出力）される状態 $|1,0\rangle$ と (−) ポートから 1 個の光子が入力（出力）される状態 $|0,1\rangle$ を確率振幅 z_+, z_- で重ね合せた状態 $|z;N\rangle$

$$|z;N=1\rangle = z_+|1,0\rangle + z_-|0,1\rangle \qquad (3.11)$$

に注目する．

まず，アリスが (+) ポートから入力する，光子 1 つの状態が，

$$|z_{in};N=1\rangle = \beta|1,0\rangle \qquad (3.12)$$

であったとする．つまり，$z_{in}=\begin{pmatrix}\beta\\0\end{pmatrix}$ である．BS1 を通過した直後の光の状態は，(3.7) 式より，

$$z'_{out} = T_x\left(\frac{\pi}{2}\right)z_{in} = \frac{\beta}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} \qquad (3.13)$$

の確率振幅で重ね合わされたものとなる．次に，この出力光を PSA に入力し，(+), (−) ポートで光の位相を $(\gamma_+,\gamma_-)=(\phi_A,0)$ と変調する．PSA から出力される光は，

$$\begin{aligned} z''_{out} &= e^{-i\frac{\phi_A}{2}}T_z(\phi_A,0)z'_{out} \\ &= \frac{\beta}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\phi_A}{2}}\\-ie^{-i\frac{\phi_A}{2}}\end{pmatrix} \end{aligned} \qquad (3.14)$$

という確率振幅で重ね合わされている．

さらに，この光はボブ側の PSB に入力される．ここでの位相変調は，$(\gamma_+,\gamma_-)=(0,\phi_B)$ であるので，PSB から出力された光の状態の重ね合わせは，

$$\begin{aligned} z'''_{out} &= e^{-i\frac{\phi_B}{2}}T_z(0,\phi_B)z''_{out} \\ &= \frac{\beta}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\Delta\phi}{2}}\\-ie^{-i\frac{\Delta\phi}{2}}\end{pmatrix} \end{aligned} \qquad (3.15)$$

によって表わされる．ただし，$\Delta\phi=\phi_A-\phi_B$ とおいた．この光がボブ側の BS2 を通過するので，

$$\begin{aligned} z_{out} &= T_x\left(\frac{\pi}{2}\right)\frac{\beta}{\sqrt{2}}\begin{pmatrix}-ie^{-i\frac{\Delta\phi}{2}}\\e^{i\frac{\Delta\phi}{2}}\end{pmatrix} \\ &= -i\beta\begin{pmatrix}\cos\left(\frac{\Delta\phi}{2}\right)\\\sin\left(\frac{\Delta\phi}{2}\right)\end{pmatrix} \end{aligned} \qquad (3.16)$$

となる．ここで，(3.15) 式の (±) ポートからの出力をそれぞれ (∓) ポートに入力していることに注意しよう．(3.16) 式より，ϕ_A と ϕ_B の差のみが最終的な出力状態に影響を与えることがわかる．

前節の (1) ～ (5) の規則に従って符合化した結果を表 1 に示す．ϕ_A と ϕ_B の差によって，$z_{out,+}$, $z_{out,-}$ の両方が値を持つ場合と，片方は 0 となる場合がある．アリスとボブの設定した位相差が 0 または π のときには，常に (+) または (−) ポートの片方のみから出力される．前述のように 0 と 1 の値を割り当てておけば，両者の位相設定を確認するだけで，確実に全く同じ乱数列を共有できるのである．

表 1　BB84 プロトコルの入出力関係

アリス		ボブ		
ϕ_A	ビット値	ϕ_B	$(z_{out,+},z_{out,-})$	ビット値
0	0	0	$\beta(-i,0)$	0
		$\frac{\pi}{2}$	$\frac{\beta}{\sqrt{2}}(-i,-1)$	
π	1	0	$\beta(0,-1)$	1
		$\frac{\pi}{2}$	$\frac{\beta}{\sqrt{2}}(-i,-i)$	
$\frac{\pi}{2}$	0	0	$\frac{\beta}{\sqrt{2}}(-i,-i)$	
		$\frac{\pi}{2}$	$\beta(-i,0)$	0
$\frac{3\pi}{2}$	1	0	$\frac{\beta}{\sqrt{2}}(i,-i)$	
		$\frac{\pi}{2}$	$\beta(0,-1)$	1

このプロトコルの安全性について考えてみよう．イブは，単一光子パルスの取扱いに習熟しているものとする．つまり，光子の検出を精密に行うことができ，かつ任意の時間，光子を貯蔵しておく能力を持っているとする．ただし，パルスの送信後に行う交信内容の変更はできないものとする．イブの戦略としては次の 2 つが考えられる：

(1)　送信中の光子を捉えて測定した後，測定結果と同種の光子をボブに送る．
(2)　BS を余分に光路中に置いておき，イブの方に出力されるようにしておく．

しかし，(1) では光子の測定を行うことによって，(2) では BS を置くことによって光子の状態が変化してしまう．ボブの受け取るデータの誤り率が変化することから，イブの存在が通信の当事者にわかってしまうのである．

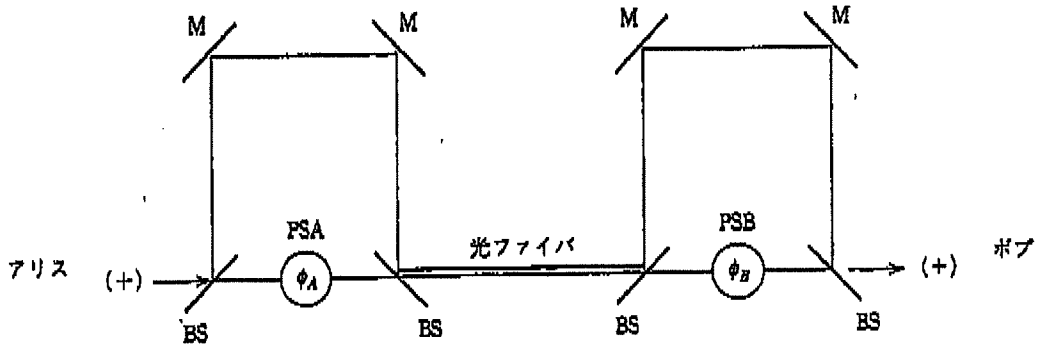


図4　B92プロトコル用の干渉計を用いた装置

4. 量子論的な暗号鍵の配布（QKD） B92プロトコル

MZ干渉計を用いたBB84プロトコルは，ただひとつの干渉計を用いているため，送信者と受信者が遠距離にいるときには実現が難しい．そこで，ベネットは新たなプロトコルを1992年に考案した[12]．まず，アリスとボブが各々干渉計を持ち，両者の間を光ファイバーで繋いでおく（図4）．

この干渉計に含まれている2つのBSは，(+)ポートよりも高い確率で光子が(−)ポートから出力されるように設定されている．最初のBSの(+)ポートから出力された光が位相シフトを受けた後，2番目のBSに到達するまでの時間が，(−)ポートからの出力光より短くなるように鏡（M）の位置を調節しておく．通信手順はBB84とほとんど同じであるが，(2),(3),(4)は以下のように変更されている．

(2)′ アリスは，常に光子1つ分程度の弱い光を(+)ポートから入力する．送信は，自分の作成した乱数列に従って，移相器で信号の位相を変調してから行う．乱数の値が0であれば，位相を0とし，1であれば，位相をπとする．

(3)′ ボブは，信号を受け取る直前に自分の作成した乱数列に従って移相器の位相を変化させる．乱数列の値が0であれば位相を0，1であればπとする．

(4)′ ボブ側では，(+)ポートからの光の出力を観測する．位相設定が0のときに出力光を検出すれば0，位相設定がπのときに検出すれば1とする．光を検出したときの，ボブ側の位相の設定と，受け取ったビット値を記録しておく．

ボブは，時間差をおいて3種類の信号を検出する．2番目の信号は，アリスとボブの位相設定が等しいときに限り出力されるので，(2)′と(3)′の規則について両者が了解していれば，位相設定をお互いに確認するだけで，同じ乱数列を共有できる．

この仕組みも，量子チャンネル理論によって解明してみよう．

4.1 理論的記述

アリスが$x_{in}=\begin{pmatrix}\beta\\0\end{pmatrix}$という状態の光を入力し，BSを通した後，$(\gamma_+,\gamma_-)=(\phi_A,0)$と位相変調することによって得られる出力光は，

$$x'_{out}=e^{-i\frac{\phi_A}{2}}\mathcal{T}_z(\phi_A,0)\mathcal{T}_x(\alpha)x_{in}=\beta\begin{pmatrix}e^{i\frac{\phi_A}{2}}\cos\left(\frac{\alpha}{2}\right)\\-ie^{-i\frac{\phi_A}{2}}\sin\left(\frac{\alpha}{2}\right)\end{pmatrix}\qquad(4.1)$$

で表わされる．

(−)ポートへの出力のほうが，(+)ポートに比べてrだけ長い光路を経ている場合には，次のような変換行列を用いればよいと思われる．

$$\mathcal{T}'_z(r)=\begin{pmatrix}1&0\\0&e^{ikr}\end{pmatrix}.\qquad(4.2)$$

ここで，kは送信する光の波数を表わす．この変換行列は本質的にPSと同等であるから，出力状態は，

$$|x_{out};N\rangle=\left|e^{-i\frac{kr}{2}}\mathcal{T}'_z(r)x_{in};N\right\rangle\qquad(4.3)$$

となる．

(4.3)式を用いて，アリス側から出力される信号は次のようになる．

表2 B92プロトコルの入出力関係

アリス		ボブ		
ϕ_A	ビット値	ϕ_B	$z_{out,+}$	ビット値
0	0	0	$-2\beta\cos^2\left(\frac{\alpha}{2}\right)\sin^2\left(\frac{\alpha}{2}\right)$	0
		π	0	
π	1	0	0	
		π	$-2\beta\cos^2\left(\frac{\alpha}{2}\right)\sin^2\left(\frac{\alpha}{2}\right)$	1

$$z''_{out} = e^{-i\frac{kr}{2}}T_x(\alpha)T'_x(r)z'_{out}$$

$$= \beta \times \begin{pmatrix} e^{-i\frac{kr}{2}}e^{i\frac{\phi_A}{2}}\cos^2\left(\frac{\alpha}{2}\right) - e^{i\frac{kr}{2}}e^{-i\frac{\phi_A}{2}}\sin^2\left(\frac{\alpha}{2}\right) \\ -i\left(e^{-i\frac{kr}{2}}e^{i\frac{\phi_A}{2}} + e^{i\frac{kr}{2}}e^{-i\frac{\phi_A}{2}}\right)\cos\left(\frac{\alpha}{2}\right)\sin\left(\frac{\alpha}{2}\right) \end{pmatrix}. \quad (4.4)$$

出力された光のうち，(+) ポートからのもののみを光ファイバーを通じてボブに送信する．最終的に，ボブ側の (+) ポートからは次のような信号が出力される：

$$z_{out,+} = e^{-ikr}z_1 + z_2 + e^{ikr}z_3. \quad (4.5)$$

ここで，z_1, z_2, z_3 は

$$z_1 = e^{i\frac{(\phi_A+\phi_B)}{2}}\cos^4\left(\frac{\alpha}{2}\right)\beta, \quad (4.6)$$

$$z_2 = -\left(e^{i\frac{\Delta\phi}{2}} + e^{-i\frac{\Delta\phi}{2}}\right)\cos^2\left(\frac{\alpha}{2}\right)\sin^2\left(\frac{\alpha}{2}\right)\beta, \quad (4.7)$$

$$z_3 = e^{-i\frac{(\phi_A+\phi_B)}{2}}\sin^4\left(\frac{\alpha}{2}\right)\beta \quad (4.8)$$

である．ここに，$\Delta\phi = \phi_A - \phi_B$ とした．r による光路差が大きく，通った道筋によってボブの検出器で検出できるくらいの時間差が生ずるとすると，ボブは，e^{ikr} の次数によって区別される3種類の信号を受け取ることになる．2番目に受け取る信号に対して前述の規則を用いて0と1の数字を割り当てた結果を表2に示す．表2より，アリスとボブの位相設定が等しいときに限り，2番目の信号が出力されることがわかる．このようにして，両者が位相設定を確認するだけで同じ乱数列を共有できるのである．

4.2 B92プロトコルの実現

さて，ここで光ファイバーを用いてB92プロトコルを実現した装置を紹介しよう[13]．これは，図4中の干渉計に相当する部分を (1) 2つの50–50カプラ，(2) 移相器，(3) 長さの違う2本の光ファイバで，構成したものである（図5）．ここに50–50カプラとは，入力光子を2つの出力端子のうちのどちらかに50%の確率で出力する，2入力2出力のデバイスで，BSの役割を果たす．移相器としては，印加電圧によって屈折率が変化する非線形結晶を用いている．2つのカプラを長さの異なるファイバで繋いでいるのは，図4の中の鏡による光路差を実現するためである．ここでは，長いファイバを通った光子は，8.5ns (=10億分の8.5秒) 遅れて次のカプラに到着するように設定してある．300 psの電気パルスをレーザーに印加して直線偏光の光を作成し強度を十分に減衰させてから，図5のアリス側のカプラの片方の端子に入力する．このとき，ボブ側の出力端子の一方に繋いである検出器（InGaAs結晶を用いた光ダイオード）が捉えた光子数の時間スペクトルを図6に示す．前節で述べたように，確かに3種類の信号が時間差（約8.5 ns）で検出されている．中心のピークはアリスとボブの位相設定によって検出されたり，されなかったりする，というわけである．

QKDの実現に際しては，この光学系を2台のコンピュータ（以下，PC）で制御する（図7）．1台は全体の時間制御とアリス側の位相設定を行い，もう1台はボブ側の位相設定と検出結果を記録するのに用いる．2台のPCをイーサネットケーブルで繋いでおき，パルス送信後，位相設定を確認する交信に用いる．実行手順は次の通りである．まず，アリスとボブが擬似乱数による乱数列を独立に作成しておく．アリス側のPCの制御のもと，各々の乱数列の値を1つずつ用いて，それぞれの移相器の設定を行う．パルス送信後，ボブ

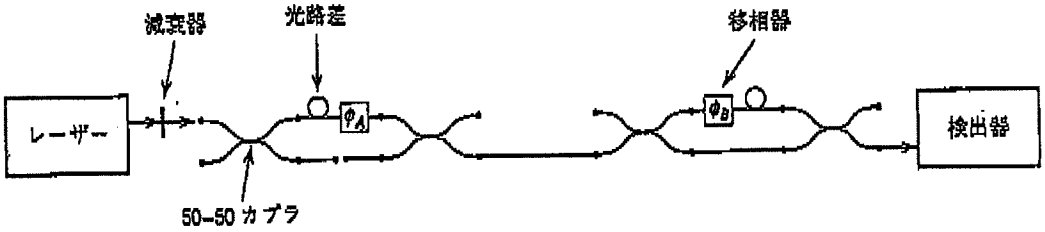


図5 光ファイバによるB92プロトコル実現装置の量子通信チャンネル部分[14]

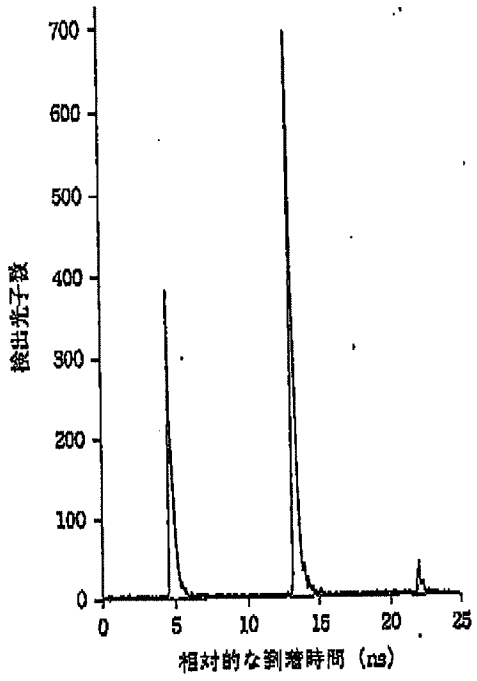


図6　ボブ側の検出器が捉えた光子数の時間スペクトル[14]

側の検出器が2番目の信号を検出したか，しなかったかを記録する．この手続きを作成した乱数列の分だけ繰り返した後，ボブは，(1) 位相設定に用いた乱数列，(2) 検出器が信号を検出したか否か，を記録したファイルをイーサネットを経由してアリス側のPCに送る．ボブ側で信号を検出したもののみを抽出することにより，暗号鍵ができあがる．

アリスからボブへの実際のメッセージの送信は，例えば次のようにして行う．アリスは，メッセージをASCIIコードに変換する．このコードと同じ長さの暗号鍵を作成して順番にメッセージコードに加える．新しいASCIIコードに対応した文字を書き込んだファイルをボブにイーサネット経由で送信する．ボブは，受け取ったファイルのメッセージコードから暗号鍵の値を引くことにより，アリスのメッセージを安全に受け取ることができるのである．

5. おわりに

本稿で紹介した量子論的な暗号鍵の配布は，量子力学の原理が実用面で直接役に立つ好例であろう．量子力学が正しければ，通信内容の機密保持が可能だ，というのである．そのポイントは，「量子力学的状態を観測すれば，必ず系が乱されてしまう」，という原理を最大限に用いたところにある．つまり，直交合わせによって作り出された量子論的な信号をやりとりしている場合，盗聴行為をするには必ずなんらかの「観測」を行わねばならず，「観測」によって系が乱されたことが必ずわかる工夫が可能となるのである．数学的な理論によって如何に解読不能な暗号が開発されても，量子力学を用いない信号伝達をしている限りは，盗聴の痕跡は残らないから，どこかで情報が漏れ，この暗号も解読されるのでは，という不安から逃れることはできない．

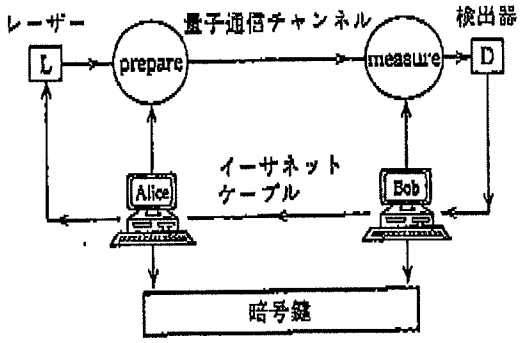


図7　B92プロトコル実現装置の全貌[14]

量子暗号系の開発にあたっては，量子力学の正当性を利用するだけでなく，その基本原理を確認するための基礎的な実験を行う必要性も生じてくるだろう．量子暗号から物理学の基礎へのフィードバックも期待できる．のみならず，理論，実験，応用物理的な研究を喚起する源泉の一つとなる可能性もある．一例として，微小共振器を用いた量子論的な1モードの光子状態の生成[18]が挙げられる．本稿で紹介した例では，量子論的な性質を持った信号を送るためにレーザー光を減衰させていたのだが，この実験装置は量子論的な光の直接的生成を可能にするものである．今後もこのような進展が望まれる．

筆者の量子暗号に対する視座は，高知大学の松枝秀明教授とお茶の水女子大学の柴田文明教授との共同研究[20]によるところが大きい．また，草稿段階で貴重なご意見を頂いた，お茶の水女子大学の柴田文明教授と山梨大学の藤間一美助教授に深謝申し上げ，本稿を終える．

参考文献

1) S. Wiesner: SIGACT News, 15 (1983) 78.
2) ディラック：量子力学（朝永振一郎，玉木英彦，木庭二郎，大塚益比古，伊藤大介訳）岩波書店（1982年），§2の訳注．
3) C.H. Bennet and G. Brassard: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.175.
4) C.H. Bennet, G. Brassard, and A.K. Ekert: *Sci. Amer.*, 267 (1992) 50.（日本語訳が日経サイエンス12月号 (1992) 50にある．）
5) C.H. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin: *J. Cryptology*, 5 (1992) 3.
6) A. Muller, J. Breguet and N. Gisin: *Europhys. Lett.*, 23 (1993) 383.
7) A.K. Ekert: *Phys. Rev. Lett.*, 67 (1991) 661.
8) C.H. Bennet, G. Brassard and N.D. Mermin: *Phys. Rev. Lett.*, 68 (1992) 557.
9) A. Aspect, P. Grangier and G. Roger: *Phys. Rev. Lett.*, 49 (1982) 91; A. Aspect, J. Dalibard and G. Roger: *ibid.*, 49 (1982) 1804.
10) A.K. Ekert, J.G. Rarity, P.R. Tapster and G.M. Palma: *Phys. Rev. Lett.*, 69 (1992) 1293.
11) A.K. Ekert and G.M. Palma: *J. Mod. Opt.*, 41 (1994) 2413.
12) C.H. Bennet: *Phys. Rev. Lett.*, 68 (1992) 3121.
13) R.J. Hughes, D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan and M. Schauer: *Contemp. Phys.*, 36 (1995) 149.
14) S.J.D. Phoenix and P.D. Townsend: *Contemp. Phys.*, 36 (1995) 165.
15) C. Marand and P.D. Townsend: *Opt. Lett.*, 20 (1995) 1695.
16) P.D. Townsend: IQEC '94 Summaries of papers presented at the International Quantum Electronics Conference, 9 (1994) 139.
17) F. Shibata and C. Uchiyama: *Physica* に投稿準備中．
18) 例えば，B. Yurke, S.L. McCall and J.R. Kaluder: *Phys. Rev.*, A 33 (1986) 4033.
19) F. De Martini, G. Di Giuseppe and M. Marrocco: *Phys. Rev. Lett.*, 76 (1996) 900.
20) H. Matsueda, F. Shibata, and C. Uchiyama: "Quantum Cryptography Modulating the Spontaneous Emission Rate of Photons" Prago Crypto '96, Ptague, Czech Republic, Sept. 30–Oct. 3.

（うちやま・ちかこ，山梨大学工学部）

特　集（1997年1月号予告）

逆問題のひろがり

定価980円

逆問題の版図と数学 微分方程式の係数決定を巡って　山本　昌宏
逆問題的問題　山田　道夫
ニアフィールド光学における逆問題　河田　聡
計測するとデータが壊れる世界の計測
非破壊評価とは何か クラック決定問題に関する話題　西村　直志
逆問題の考え方と枠組 工学的側面を中心として　久保　司郎
地球の内部を探る　谷本　俊郎
いくつかの凸な物体による散乱　井川　満
物体による散乱の数値解析　大西　和榮
非適切問題の数値解析　磯　祐介

特　集（1996年11月月号）

計算物理学最前線

シミュレーションによる物理

定価980円

計算物理学の進展とその背景　岩崎　洋一
素粒子物理学とシミュレーション　宇川　彰
数値的方法による格子上の場の理論
物性物理とシミュレーション　高山　一
宇宙物理学とシミュレーション　観山　正見
流体力学とシミュレーション　長野　靖尚　大宮司久明
気象の予測とアジョイント・モデル　露木　義
ニューラルネットワークとシミュレーション　西森　秀稔
最適化と蛋白質の立体構造予測シミュレーション　岡本　祐幸

〈量子力学とは何か⑭〉 量子力学ミニマム(14)　高林　武彦
〈研究室の窓〉 エルニーニョカオス　木本　昌秀
文化財を読み解く科学　村上　陸

編集後記

人類が農耕を始めてから現在までのタイムスケールで見れば，17世紀の「微分積分」発見はついこの間の出来事だろう．微分積分は，科学革命・古典力学の成立という，誇るべき「誕生の物語」を持っている．しかし，無限小に対する先駆的な考察がそれ以前にもあることからも明らかなように，微積分という知の持つ普遍性は，人類の歴史全体から理解されるべきなのだろう．その普遍性は，芸術の「芸」の字の源義である，農耕・生産に関わるひとつひとつの技術・知恵の集積，そういったものと，遠いところでつながっているような気がする．共に，自然の認識の方法，問題解決の処方，内在的な合理性を備えているという意味で．

高校生から読める連載「微分積分」が今月からいよいよ始まる．乞御期待．
（平勢）

今年一年を振り返ると本当にいろいろなことがありました．季節の移り変わりが確実に時間がたっていることを教えてくれます，それがとてもつらいということも知りました．

悲しいこと，つらいことがあって精神的に弱くなっているとき，気がつくとまわりで暖かく見守っている人たちがいました．この一年は，多くの人たちに支えられているのだとあらためて感じた年でもあります．私のことを心配して京都から駆けつけてくれる友達や，いつでも暖かく受け入れてくれる人たち，何も言わないけどいつも側で見守ってくれる人に囲まれ，支えられています，まわりの暖かい心遣いが私を元気づけ，励ましてくれました．
（米沢）

数　理　科　学　12月号

1996年12月1日発行

発行人　森　平　勇　三

数理科学編集部
TEL.(03)5474-8816
FAX.(03)5474-8817
ホームページ　http://www.bekkoame.or.jp/~saiensu
ご意見・ご要望は　saiensu@lib.bekkoame.or.jp　まで．

企画・編集スタッフ　平勢耕介・田島伸彦
米沢美由樹・竹田　直

発行所　© 株式会社サイエンス社
〒151　東京都渋谷区千駄ヶ谷1-3-25　振替00170-7-2387
TEL.(03)5474-8500（代表）
(03)5474-8700(広告部)

印刷・製本　三美印刷株式会社　山岡景仁